

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

Listing of Claims:

Claims 1-38 (Cancelled).

Claim 39 (New): A method for securing scrambled data supplied to a plurality of receiver terminals, each of the terminals having a plurality of different descrambling modules, each descrambling module having a specific processing capacity and a specific level of security, the data being previously subdivided into M families, each family comprising N blocks, the method comprising:

assigning to each family an identification parameter,

defining a biunivocal relation between the identification parameter of each family with a key K defined as a function of the specific processing capacity and the level of security of the descrambling modules for descrambling the blocks of said family,

scrambling, at transmission, each block of a family by the key K associated with the identification parameter of the family, and

descrambling, at reception, each block of a family by the descrambling module corresponding to the key associated with the identification parameter of said family.

Claim 40 (New): The method as claimed in claim 39, wherein the descrambling modules are different peripheral elements associated with the receiver terminals.

Claim 41 (New): The method as claimed in claim 40, wherein the descrambling modules comprise different algorithms.

Claim 42 (New): The method as claimed in claim 39, wherein the data to be distributed are in the form of a previously stored file.

Claim 43 (New): The method as claimed in claim 39, wherein the data to be secured are in the form of a broadcast or downloaded stream and processed in real time by the terminal.

Claim 44 (New): The method as claimed in claim 43, wherein the duration of use of the stream is divided into crypto periods, each corresponding to a descrambling key, and in that prior to each start of the crypto period a message is inserted into the stream so as to warn the descrambling module of the change in the crypto period.

Claim 45 (New): The method as claimed in claim 44, wherein said message comprises all information necessary for descrambling the stream utilized during the following crypto period.

Claim 46 (New): The method as claimed in claim 39, wherein said data represent at least one of audio or video programs protected by a DRM system.

Claim 47 (New): The method as claimed in claim 39, wherein said data represent images synthesized images.

Claim 48 (New): A system for securing scrambled data supplied to a receiver terminal comprising a plurality of different descrambling modules, each descrambling modules having a specific processing capacity and a specific level of security, the data being

previously subdivided into M families, each family comprising N blocks, the system comprising:

- a scrambling device configured to
 - assign to each family an identification parameter,
 - define a biunivocal relation, between the identification parameter of each family with a key K defined as a function of the specific processing capacity and the level of security of the descrambling modules for descrambling the blocks of said family, and
 - scramble, at transmission, each block of a family by the key K associated with the identification parameter of the family; and
- a descrambling device configured to identify the family of each block so as to descramble each block of a family by the descrambling module corresponding to the key associated with the identification parameter of said family.

Claim 49 (New): The system as claimed in claim 48, wherein the descrambling modules are distinct peripherals associated with the receiver terminal.

Claim 50 (New): A scrambling device for a stream of data that is configured to:

- subdivide said stream into M distinct families of N blocks,
- assign to each family an identification parameter,
- define a biunivocal relation between the identification parameter of each family with a key K defined as a function of the specific processing capacity and the level of security of the descrambling modules for descrambling the blocks of said family, and
- scramble, at transmission, each block of a family by the key K associated with the identification parameter of the family.

Claim 51 (New): The descrambling device as claimed in claim 50, further comprising:

means for identifying the family of each block so as to descramble each block of a family by the descrambling module corresponding to the key associated with the identification parameter of said family.

Claim 52 (New): The descrambling device as claimed in claim 51, further comprising:

a plurality of distinct descrambling modules each identified by the specific identification parameter.

Claim 53 (New): The descrambling device as claimed in claim 52, wherein the receiver terminal is a PDA and one of said descrambling modules is integrated into the PDA and at least a second module is a smart card of SIM type connected to said PDA.

Claim 54 (New): The method as claimed in claim 39, further comprising:
securing a video-on-demand service (VOD) by said step of scrambling.

Claim 55 (New): The method as claimed in claim 39, further comprising:
securing a music-on-demand service (MOD) by said step of scrambling.

Claim 56 (New): The method as claimed in claim 39, further comprising:
securing access to a broadcast service for electronic books online or downloaded from portable media by said step of scrambling.